タイトル　人類が絶滅する 6 のシナリオ

原　　題　**THE FATE OF THE SPECIES**

著　　者　**Fred Guterl(フレッド・グテル)**

訳　　者　夏目　大（なつめ　だい）

出 版 社　河出書房新社

発 売 日　2013 年 9 月 20 日

ページ数　318 頁

図書館の新刊書のコーナーで「もはや空想ではない終焉の科学」という過激なタイトルの本が目に留まった。トンデモ本かなと思い中身を覗いてみると、著者は「サイエンティフィック・アメリカン誌（日経サイエンスの親雑誌)」の編集長なので、そうではなさそうだ。しかも、著者にとっては本書が初の著書だという。

原題は THE FATE OF SPECIES（人類の運命)、副題は Why the Human Race May Cause Its Own Extinction and How We Can Stop It（何故人類は絶滅に至るかもしれないのか、どうすればそれを止めることが出来るか）である。

私たちは、漠然とした不安を抱えて生きている。最も大きい不安と言えば「近いうちに人類は滅びるのではないか」という不安である。今現在は繁栄を謳歌しているけれども、こんなことは何時までも続くはずがないのではないか、近い将来、悲惨なことが起きるのではないか、という不安である。

問題は、悲惨なことが具体的に何なのか、気が付かないうちに事態が悪化していき、滅亡に近づいているかも知れないと思うとやはり不安である。

本書は、その不安の原因を少しでも明確にしようという姿勢で、「人類にとって最悪の場合、何が起こりうるか」、その可能性を 6 つのシナリオに分けて論じている。

人類が滅亡するとすれば、科学・技術の発達が原因になる可能性が高い。そうであるならば、「科学はもう発達しなくてもいい」、「科学・技術が発達する以前のように、自然と共に暮らすべきではないだろうか」という人もいる。

しかし著者は、科学・技術の発達が我々を追い込んだのは確かだが、だからといって、科学・技術を放棄すれば良いというわけではない。窮地を脱するには、やはり科学・技術をさらに発達させるしか方法はないと著者は主張する。何故なら、もう後戻りできないからだという。

さて、最悪の 6 つのシナリオとは何だろう。以下、タイトルを見てみよう。

第1章　世界を滅ぼすスーパーウィルス
第2章　繰り返される大量絶滅
第3章　突然起こり得る気候変動
第4章　生態系の危うい均衡
第5章　迫りくるバイオテロリズム
第6章　暴走するコンピューア
終りに――　創意工夫のみが人類を救う

である。

第 1 章では、章の初めの河岡義裕教授（現東京大学医科学研究所）の話が出て来る。氏が、アメリカ、テネシー州にあるインフルエンザ研究室へポスドクに推薦されたところからこの章は始まる。

インフルエンザは、2009 年に流行し、一時大騒ぎになったが、結局致死率の低いもので大事に至らなかった。ただ、インフルエンザのウィルスは、ほんの少し遺伝子の配列が違っていれば、全世界に破滅的な被害をもたらす恐れがあったという。

第 2 章では、生物の大量絶滅が考察されている。地球上の生物は大量絶滅に向かっていると主張する人もいる。果たしてそれは本当なのかを過去の大量絶滅とも対比しながら考察している。もし、生物の大量絶滅がすでに始まっていて、それを止める方法がないのだとしたら、人類も必ず同時に滅亡するはずだという。

第 3 章では、気候について触れている。地球の気候は今後、急激に悪い方に変化してしまう可能性がある。その変化は、多くの科学者が予測しているよりもずっと早く始まるかも知れないという。気候が大きく変化すれば、人類をはじめとする生物は絶滅の危機に追い込まれる。生物は皆、環境の微妙なバランスの上で生きているのだが、そのバランスが崩れてしまうからだ。どうすれば、この気候変動を食い止められるのかに言及する。

第 4 章では、生態系について考察する。人間は、食物連鎖の中でも特殊な位置を占めており、そのおかげで繁栄してきた。しかし、いま、人間の食糧は非常に危うい状態に置かれている。病気や、ちょっとした環境の変化で農作物の供給が急に途絶える恐れがあるからだ。

第 5 章では、合成生物学について取り上げている。バイオテクノロジーの進歩により、人類はついに自らの手で思い通りの生物を作る能力を手に入れた。ただ、この能力を悪人が使うと、恐ろしい病原体が産み出され、人類が滅亡する危険性がある。

第 6 章に書かれているのは、インターネットなどのハイテクに依存することの危うさである。快適な生活を送れる反面、コンピュータの動作はごく少数の悪人によるサイバー攻撃で簡単に攪乱されてしまう。コンピュータの更なる進歩で、近い将来、人間と同じように思考し、行動する機械が生まれることも有り得る。そうした機械は人類にとって役立つ

ものであると同時に、人類と敵対する危険性も秘めている。
「終わりに」では、人類が現代直面している危機をどうすれば回避できるかを考察している。本書で問題にしたのは、多くは科学・技術の発達が招いた危機だが、科学・技術の発達を止めるということは解決にならない。我々は、科学・技術をより発達させ、上手に利用することでしか、困難を乗り越えられないと結論付けている。

さて、どの章も衝撃的だが、第 6 章の「暴走するコンピュータ」が最も衝撃的であった。
中身を少し覗いてみるが、その前に、本章で頻繁に出て来る、「マルウェア」と「スタックスネット」について述べておこう。
まず、「マルウェア（Malware)」とは、悪意のあるという意味の Malicious と Software を組み合わせて作られた合成語で、「不正で有害な動作を行う意図で作られた悪意あるソフトウェア」を指す。
一方、「スタックスネット（Stuxnet)」は Microsoft Windows で感染するコンピュータウィルスである。このソフトは、インターネットから隔離されたスタンドアローンの産業用制御システムにおいても感染し、かつ実害を生じるという特徴がある。
もう一つ付け加えておくと、AI から派生した言葉で、「機械が人間の介入なしに自ら判断を下す」時に使う言葉で「自律的」という言葉がある。このスタックスネットは、すべての意思決定を「自立的」に行うところに特徴がある。
さて、スタックスネットはやみくもにコンピュータからコンピュータへと感染していくのではなく、特定のターゲットにじわじわと近づいていく能力を持ったマルウェアである。
2010 年に報告された標的はイランにあるウラン濃縮用の分離機を制御するコンピュータであった。そして実際に遠心分離器の制御コンピュータに侵入することに成功し、侵入した後は遠心分離器のロータの回転を少し上げただけだった。しかも、現場の技術者が気付かない程度に、しかし気付いた時には遠心分離機は壊れているという仕掛けになっていた。
制御コンピュータには、正常に動作しているというスタックスネットにより捏造されたウソのデータが表示されるように仕組まれていた。マルウェアが遠心分離機を制御するコンピュータにたどり着き、それを破壊するまでの手順に人間は全く関与しないでもっぱらマルウェアが自律的に行っていたというわけである。
代替手段があるうちは、ほぼ影響はないと言っても良いが、深刻な影響が出るのは、何もかも奪われ、代替手段が無くなってからだという。そうなったらまさに悪夢である。
スタックスネット侵入以後、ウラン濃縮施設に起きた惨事について、イランは詳しい情報を公開してはいない。
ニューヨーク・タイムズは、NSA(アメリカ国家保安局)とイスラエル軍の情報機関（Unit8200）が、このマルウェアをイラン攻撃用に作ったと報じている。また、スノーデンも NSA とイスラエルが共同で開発したと語っている（Wikipedia)。
イランを攻撃した高度なマルウェアを作れる国は世界に 20 程あるとされている。現状で

は、一定以上の規模の軍需産業のある大国の機関でなくては作れそうもないが、あと 20 年もすれば、もっと幅広い層の人達が同等のマルウェアを作れるようになるはずだという。

本書には、原子力発電に関する事故は出てこなかった。日本では現実に起きてしまった事故に対して、「原発推進派」と「反原発派」の不毛な対立が今現在も続いている。

「原子力発電をどうするか」という問いへの答えとしては、「これまで通り推進」と「現在動いている原子炉を全て廃炉にする」の両極端の間に、無数の選択肢があるはずである。

日本では何時でも二分法的思考が主流を占めている。二分法的思考に共通しているのは、科学がグレーな領域で少しずつマシな方向に進むものだということを見失っていることである。

さて、原発と言っても電力会社である。電力会社と政府は、配電網とインターネットの接続を積極的に推進しているだろうから、マルウェアに対する脆弱性が大幅に上がることになるだろう。配電網に感染できるマルウェアは、某国の諜報員が USB メモリやメールの添付ファイルを使って拡散させることは簡単である。本章にもその手口が詳しく紹介されている。

日本の配電網には既に何らかのマルウェアが侵入しているかも知れない。侵入だけさせておいて、いずれ必要となった時に作動させるかも知れない。コンピュータ制御による機械システムは全てこのような弱点がある。

2003 年アメリカ北東部で発生した大停電も、日本にも無縁ではない。アメリカでは、マルウェアが起こす停電のシミュレーションさえ行っている。日本で起これば、日本の大部分が少なくとも数か月間、電力無しという状況になるのではないか？

日本も、重要なインフラに関しては、机上のシミュレーションをやるべきである。本書でも、サイバー攻撃によって重要なインフラに被害を受けると、社会は世界恐慌時の 10 倍くらいの悲惨な状況に陥るという。

著者の考える最悪のシナリオはマルウェアに攻撃されても、その攻撃を確実に回避できる方法が全く見つからない。さらには攻撃に対する防御を固めることも出来ない。その上コンピュータがそのマルウェアに感染しているかどうかを正確に見分ける方法もない。このような状況に陥るのが最も恐ろしい。

日本でもつい最近、中国検索最王手「百度（バイドゥ）」製の日本語入力ソフトを使用するとパソコンに入力した全ての文字情報が同社のサーバーに転送されることが判り、内閣官房セキュリティーセンターや文部科学省は、中央省庁や大学、研究機関など約 140 機関に使用停止を呼びかけている。外務省の他、東京大など少なくとも 12 大学の一部パソコンに導入されていることが判明している。

問題になっているソフトは「バイドゥ IME」で、2009 年に公開されたフリーソフトで、日本国内で約 200 万人が使用しているという。

このソフトを初期設定のまま使用すると、パソコンで打ち込んだメールや検索の単語、文書編集ソフトで作成した文書など、すべての文字列が自動的に同社のサーバーに送信さ

れるという。サーバーが中国にあるとすれば、悪用された場合に対応できないという（読売新聞 2013.12.27）。

こういうことを考えると、フリーだからとの理由で公的機関や研究機関の業務では使用するのは問題である。

・・・と書いているうちに、私自身のコンピュータのマイクロソフト IME の具合がおかしくなった。何だろうと入力モードの「設定」を見ると、「百度（バイドゥ）」製の日本語入力ソフト Baid IME 3.5 に切り替わっていた。ソフトの削除情報を見てみると 2013 年 12 月 20 日にインストールしたとある。しかし、インストールした記憶が全くないので早速削除した。入力モードから Baidu IME 3.5 は消えたが、中国製の悪事を働くとんでもないソフトが知らない間にインストールされていた。読者の皆さんも入力モード「設定」の項を確認することをお薦めする。

現状では、未知のマルウェアを発見するようなソフトウェアは開発できないと言われている。仮にマルウェアが一つ見つかったとしても、台所のゴキブリのように、すでにネットワーク上の多数のコンピュータに広がっている可能性が高い。

マルウェアが存在して悪事を働いている恐れがあると判断して捜索を開始しても、マルウェアの最初の仕事が、発電機を爆発させること、銀行のオンラインシステムを停止させること、あるいはミサイルの進路を反転させることだったとしたら、どうだろう。もう手遅れである。

「コンピュータを作るということは、ウィルスの培地を作るようなものだ」という言葉で 6 章を閉じている。

さらに、今になって科学・技術を敵視し、自然回帰を訴えたところで大した意味はない。問題を自分たちの創意工夫で解決していく、それこそが人間らしい姿と言える。幸い私たちはこれまでのところ、あらゆる逆境に打ち勝っている。これからも勝ち続けるためには、良いと思えるアイデアは全て取り入れるべきだろう。という言葉で筆者は本書を閉じている。

我々の住む世界は脆弱性を高める方向へと一直線に進んでおり、思いの外脆弱であることが判った。人類の将来は、「科学・技術の更なる発展」と「人間の良識」にかかっているとよく言われるが、悪意を持った人間たちにとって、知識さえあればスタックスネットのようなものを作ってしまえば世界を乗っ取ることさえ可能な世の中になってしまった。

先ほどの例のように、悪意を持った人間が絶えることはないことを考えると、「人間の良識」には殆ど期待できないだろう。

日本では、「人間性善説」が主流で、騙されやすい国民性が国際社会ではマイナス要因だが、欧米のように、「人間性悪説」にもう少し理解を示しても良いのではないだろうか。それにしても、恐ろしい時代に突入したものだ。

2013. 12. 28